Claims

What is claimed is:

1. A method of selecting a cryptographic strength for at least one application, in accordance with a framework for providing cryptographic support of the at least one application, comprising the steps of:

performing data encryption at a first cryptographic strength when the at least one application is privileged to perform encryption at a first cryptographic strength; and

performing data encryption at a second cryptographic strength when the at least one application is not privileged to perform encryption at the first cryptographic strength, wherein the first cryptographic strength is stronger than the second cryptographic strength.

2. The method of claim 1, further comprising the steps of:

initializing the framework to provide cryptographic support for the at least one application; and

creating a cryptographic context for the at least one application.

3. The method of claim 2, wherein the step of initializing the framework comprises the steps of:

reading at least one configuration file comprising cryptographic strength information;

determining if the at least one configuration file is signed;

returning an error that the framework failed to initialize when the at least one configuration file is not signed; and

extracting and remembering at least one second cryptographic strength value when the at least one configuration file is signed.

4. The method of claim 3, wherein the cryptographic strength information comprises key lengths at which at least one algorithm is considered at the first cryptographic strength.

5. The method of claim 2, wherein the step of creating a cryptographic context comprises the steps of:

providing an algorithm identification, a key and a key length to the at least one application;

setting the cryptographic context to the second cryptographic strength at the at least one application; and

returning an integer to the at least one application referring to cryptographic parameters.

6. The method of claim 5, wherein the step of setting the cryptographic context to the second cryptographic strength comprises the step of setting a first cryptographic strength flag to false in the cryptographic context.

7. The method of claim 5, wherein the integer comprises a cryptographic context handle.

8. The method of claim 1, wherein the step of performing data encryption at a first cryptographic strength comprises the step of determining if the at least one application is privileged to perform encryption at a first cryptographic strength.

9. The method of claim 8, wherein the step of determining if the at least one application is privileged to perform encryption at the first cryptographic strength comprises the steps of:

determining if application credentials are signed; and

returning an error of invalid credentials when the credentials are not signed.

10. The method of claim 8, wherein the step of determining if application credentials are signed comprises the step of matching a public key embedded in the framework and a private key in the at least one application.

11. The method of claim 8, wherein the step of determining if the at least one application is privileged to perform encryption at the first cryptographic strength comprises the steps of:

extracting a privilege set from credentials of the at least one application;

determining if the extracted privilege set comprises privileges defined by the framework;

returning an error when the extracted privilege set does not comprise privileges defined by the framework; and setting the cryptographic context to the first cryptographic strength when the extracted privilege set comprises privileges defined by the framework.

12. The method of claim 1, wherein the step of performing data encryption at the first cryptographic strength comprises the steps of:

receiving an integer referring to cryptographic parameters and a data buffer to be encrypted from the at least one application;

determining if the requested cryptographic strength is greater than a second cryptographic strength;

encrypting the data buffer with the second cryptographic strength when the requested cryptographic strength is not greater than the second cryptographic strength;

determining if the cryptographic context is set to the first cryptographic strength when the requested cryptographic strength is greater than the second cryptographic strength;

encrypting the data buffer with the first cryptographic strength when the cryptographic context is set to the first cryptographic strength; and

returning an error that the at least one application is not privileged for the first cryptographic strength when the cryptographic context is not set to the first cryptographic strength.

13. The method of claim 1, further comprising the step of providing an exemption mechanism for the at least one application.

14. The method of claim 1, wherein the at least one application is a common data security architecture at least one application.

15. The method of claim 1, wherein the framework is a common data security architecture framework.

16. A system for selecting a cryptographic strength for at least one application, the system comprising:

an at least one application requiring cryptographic support; and an application framework, coupled to the at least one application by an application program interface, operative to: (i) perform data encryption at a first cryptographic strength when the at least one application is privileged to perform encryption at a first cryptographic strength; and (ii) perform data encryption at a second cryptographic strength when the at least one application is not privileged to perform encryption at the first cryptographic strength, wherein the first cryptographic strength is stronger than the second cryptographic strength.

17. The system of claim 16, wherein the application framework is further operative to:

initialize the framework to provide cryptographic support for the at least one application; and

create a cryptographic context for the at least one application.

18. The system of claim 16, wherein performing data encryption at a first cryptographic strength comprises determining if the at least one application is privileged to perform encryption at a first cryptographic strength.

19. The system of claim 16, wherein determining if the at least one application is privileged to perform encryption at the first cryptographic strength comprises:

extracting a privilege set from credentials of the at least one application;

determining if the extracted privilege set comprises privileges defined by the framework;

returning an error when the extracted privilege set does not comprise privileges defined by the framework; and

setting the cryptographic context to the first cryptographic strength when the extracted privilege set comprises privileges defined by the framework.

20. The system of claim 16, wherein performing data encryption at the first cryptographic strength comprises:

receiving an integer referring to cryptographic parameters and a data buffer to be encrypted from the at least one application;

determining if the requested cryptographic strength is greater than a second cryptographic strength;

encrypting the data buffer with the second cryptographic strength when the requested cryptographic strength is not greater than the second cryptographic strength;

determining if the cryptographic context is set to the first cryptographic strength when the requested cryptographic strength is greater than the second cryptographic strength;

encrypting the data buffer with the first cryptographic strength when the cryptographic context is set to the first cryptographic strength; and

returning an error that the at least one application is not privileged for the first cryptographic strength when the cryptographic context is not set to the first cryptographic strength.